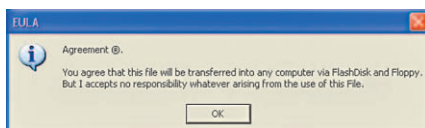
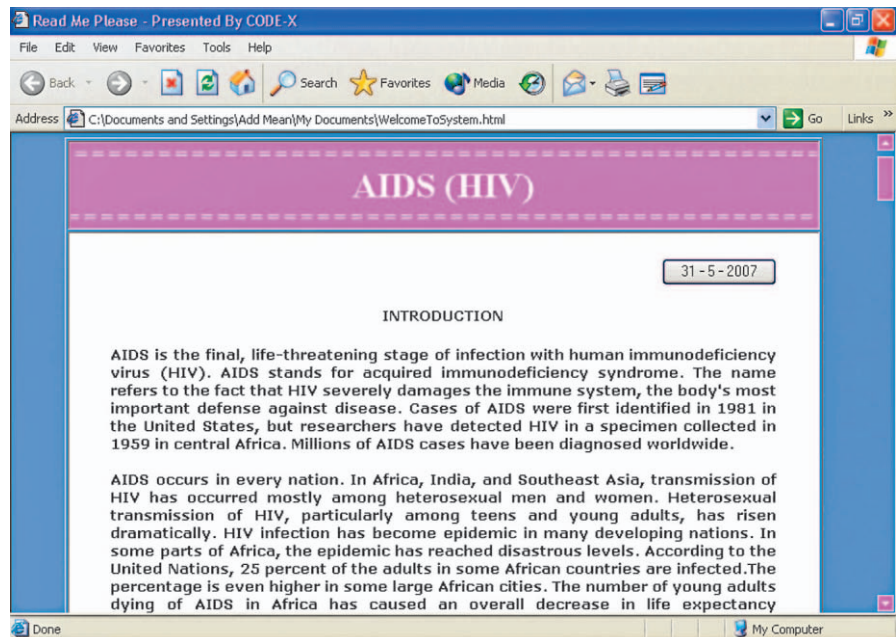
Pengenalan AIDS oleh Codex

Banyak yang menduga bahwa pembuat virus ini merupakan korban dari penyakit AIDS. Alasannya karena virus ini menampilkan pesan seputar informasi penyakit yang mematikan tersebut. Cukup beralasan, tapi terlepas dari hal tersebut, virus ini juga sudah memakan banyak korban.

Arief Prabowo

Mungkin maksudnya baik, tapi tetap saja virus ini telah mengganggu jalannya operasi komputer. Virus yang menggunakan icon Msword ini diyakini juga sebagai virus lokal, ini bisa dilihat dari string–string yang terdapat pada tubuh sang virus. Secara teknikal, virus ini memiliki ukuran yang cukup besar, pada contoh kali ini, dua buah varian yang kami punya memiliki ukuran file sebesar 253.952 bytes, cukup besar untuk ukuran sebuah virus. Virus yang dapat menyebar melalui media penyimpan data ini tidak dikompres ataupun dienkripsi, jika dilihat menggunakan hex editor akan terlihat string–string yang terdapat pada tubuh virus.

Virus ini juga akan menginfeksi setiap root drive yang ditemukannya pada komputer korban, biasanya terdapat dua buah file HTML, yakni AboutAIDS.htm, Introduction.htm, dan dua buah file executable dengan nama TIPS.exe dan %UserName%.exe (%UserName% di sini merupakan nama user yang sedang login saat itu). Pada antivirus lain, ia dikenal juga dengan nama VB.bw atau bahkan ada antivirus yang mendeteksi salah satu varian dari virus ini sebagai Small.KL? Kenapa bisa begitu ya? Padahal sudah jelas bahwa virus ini berbeda dengan Small.KL.

EULA ciptaan Codex.

AIDS Introduction yang disampaikan oleh Codex.

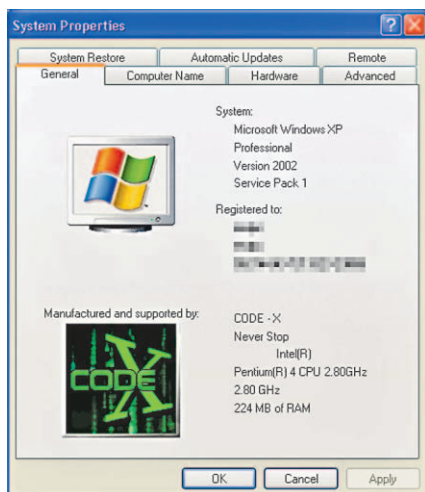
Pada saat kali pertama dijalankan, virus ini akan menampilkan *message box* yang menyatakan tentang suatu perjanjian atau EULA (End User License Agreement) seperti yang sering ditampilkan pada saat Anda menginstal software, namun bedanya yang ini ngawur, bagaimana mungkin virus ada perjanjiannya? Itu hanya "permainan" sang virus saja.

Virus ini juga akan selalu menampilkan apa yang ia namakan "Message Of The Day", biasanya pesan ini muncul pada saat start Windows, yakni pesan–pesan kata mutiara yang disampaikan oleh sang empunya virus berupa file HTML, yang ditampilkan pada *browser*. Pada system yang terinfeksi coba lihat direktori My Documents, pasti akan ada beberapa file dengan type HTML yang dibuat oleh virus di antaranya dengan nama AllMyLifeToLive.htm, WelcomeToSystem.htm, ataupun yang lainnya karena nama–nama file tersebut mungkin akan berbeda di setiap varian.

Seperti yang diutarakan di awal, virus ini juga akan menampilkan informasi seputar penyakit AIDS dengan pesan "AIDS Introduction"-nya. Apakah pembuat virus ini mengidap penyakit tersebut? Hanya ia yang tahu.

Virus juga akan mengubah atau menambahkan OEM information pada System Properties, dengan mengubah atau menambahkan file oeminfo.ini dan oemlogo.bmp pada direktori sistem Windows. Ditambah lagi, pembuatnya juga menyampaikan sedikit pesan pada *comments* yang terdapat di Version Information virus ini, "Best Variant Will Be Released (As Soon As I Can)", ini bisa Anda lihat dengan mengklik kanan file virus>Properties>pilih tab Version>lalu klik comments. Akankah muncul varian baru dari virus ini?

Registry, Sasaran Empuk

Setelah aktif di memory, dengan sigap sang virus langsung mengubah setting-an registry. Di antaranya dengan menambahkan beberapa item pada run sections agar sang virus selalu dieksekusi pada saat start Windows, dalam modus normal ataupun safe mode. Tak hanya itu, seperti yang dilakukan virus lain, ia juga akan mengubah setting-an dari Folder Options agar tidak menampilkan file atau folder dengan attribut *hidden* dan

OEM information yang diubah atau dibuat oleh Codex.

system. Virus juga mengubah *title* Internet Explorer dari "Microsoft Internet Explorer" menjadi "Presented By CODE-X", dan mengubah halaman default dari IE agar mengarah ke file yang sebelumnya telah dibuat oleh si Codex pada direktori My Documents, yakni WelcomeToSystem.htm.

Tidak seperti kebanyakan virus lainnya, yang selalu men-*disable* Regedit, Task Manager, MsConfig, ataupun Command Prompt, tapi pada virus Codex ini hal tersebut tidak dilakukan. User masih dapat mengakses tools tersebut. Ini berarti tidak menutup kemungkinan, bahwa virus ini dapat dimusnahkan secara manual menggunakan tools bawaan Windows tersebut.

Ada satu hal yang menarik di sini. Pada saat virus aktif, apabila sang user ingin mencoba untuk menghapus startup item virus dari registry menggunakan Regedit (Registry Editor) misalnya, sang virus akan langsung menutup aplikasi Regedit tersebut dan menampilkan alert pada browser Anda yang menyatakan bahwa Anda tidak boleh menghapus registry ataupun process si virus. Jadi, sebelum virus ini "mati" dari memory, startup item virus tidak akan bisa dihapus, karena virus juga akan secara terus menerus menginfeksi registry. Ini bisa dilakukan karena dalam memprogram, sang pembuat virus menggunakan *timer*, dan timer yang mengatur tentang proses tersebut ia namakan TimerReadWriteReg.

Virus Process

Virus akan menetap di memory, hanya saja apabila baru kali pertama dieksekusi, ia hanya membuat satu *process*. Baru setelah komputer di-*restart*, dengan sebelumnya telah mengubah registry, maka virus tersebut akan memiliki beberapa process.

Walaupun Task Manager tidak di-disable, tapi cukup sulit untuk mematikan virus ini. Seperti pada sampel yang kami punya, virus ini memiliki tiga process utama, yakni AllMyLifeToLive.exe, LiveForever.exe, dan WelcomeToSystem.exe. Kedua file tersebut merupakan induk dari sang virus yang ditanam pada direktori My Documents dengan ber-attribut hidden dan system. Apabila salah satu dari process tersebut di-*kill*, pasti akan muncul kembali, karena process yang satu dengan yang lainnya memiliki keterkaitan. Artinya process–process tersebut saling memanggil.

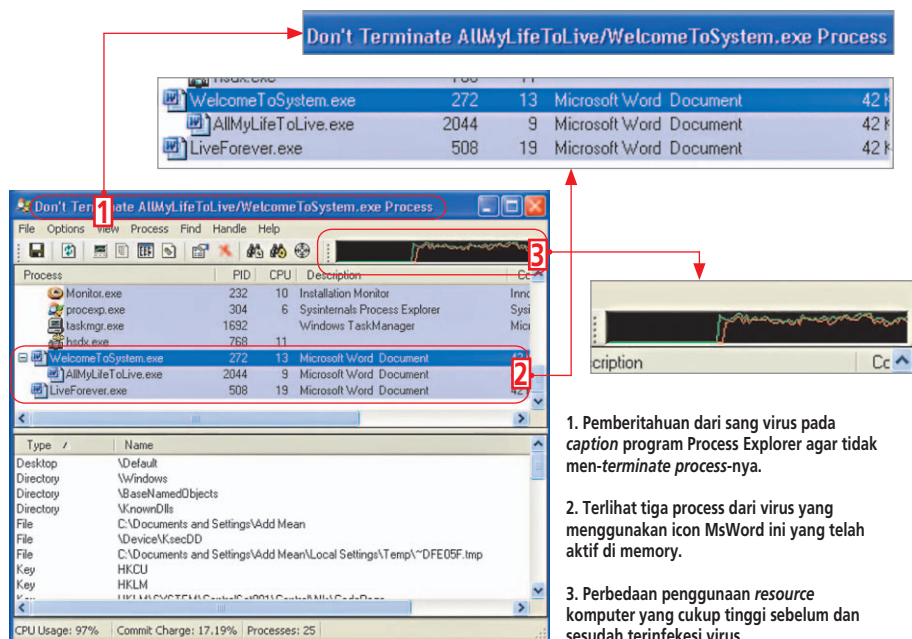
Sebenarnya ada cara yang mudah untuk meng-kill process–process tersebut, yakni dengan menonaktifkan sementara file MSVBVM60.DLL milik Visual Basic. Caranya bisa dengan me-*rename* nama file tersebut, lalu cobalah untuk meng-kill process virus tersebut. Hati–hati dengan trik ini karena dapat mengakibatkan *crash* aplikasi Visual Basic lainnya.

Virus juga memonitor program–program apa saja yang dijalankan. Apabila program tersebut dianggap mengganggu jalannya sang virus, misalnya program yang dapat meng-kill process seperti Process Explorer dari SysInternals, maka pada *caption* program tersebut akan berubah menjadi "Don't Terminate AllMyLifeToLive/WelcomeToSystem.exe Process". Itu karena virus memiliki data program–program tersebut, walaupun tidak banyak.

Untuk *services*, Windows XP contohnya, pada Control Panel>Administrative Tools>Services akan terlihat beberapa service baru, namanya bisa berupa crlxss, logsxvr, PerfLogCom, NtmsFwd, atau SrvNTs. Sepertinya virus ini mencoba meregister dirinya sebagai service, namun service yang dibuat tidak dapat berjalan dengan sempurna.

Apabila diperiksa agak lebih mendalam, virus ini diprogram menggunakan 11 komponen timer, timer ini akan bekerja secara *real-time*, yang masing–masing timer mempunyai tugas yang berbeda–beda. Inilah yang bisa mengakibatkan terkurasnya *resource* dari komputer, apalagi Codex ini tidak hanya memiliki satu process.

Pembasmian manual dari virus ini masih mungkin dilakukan, seperti yang diutarakan di atas, bagaimana cara meng-kill virus ini. Lalu setelah memory bersih dari virus, kita dapat menghapus semua startup item yang dibuat oleh virus, dan menghapus semua file virus dengan men-*search*-nya di setiap drive.

Namun, hal tersebut mungkin susah dilakukan oleh orang awam. Untuk itu, kami telah meng-update PCMAV agar dapat mengeliminasi virus ini. PCMAV sudah dapat mengenali dan membasmi dua varian dari virus ini dengan baik. Silakan scan komputer Anda dengan PCMAV RC5 ini. Apabila PCMAV tidak bisa mendeteksi virus Codex yang menyerang komputer Anda, silakan kirimkan sampelnya kepada kami. Kami tunggu. ■

1. Pemberitahuan dari sang virus pada *caption* program Process Explorer agar tidak men-*terminate process*-nya.

2. Terlihat tiga process dari virus yang menggunakan icon MsWord ini yang telah aktif di memory.

3. Perbedaan penggunaan *resource* komputer yang cukup tinggi sebelum dan sesudah terinfeksi virus.